IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JENNA WILKINSON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No. 1:19-cv-08176**
v.	)	
JUUL LABS, INC.,	)	
Defendant.	)	

FIRST AMENDED COMPLAINT

Plaintiff Jenna Wilkinson ("Plaintiff" or "Wilkinson") by and through her attorneys, individually and on behalf of all others similarly situated (the "Class"), brings the following Class Action Complaint ("Complaint") pursuant to Rule 23 of the Illinois Rule of Civil Procedure, against JUUL Labs, Inc. ("JUUL" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. JUUL is a Delaware company that manufactures electronic cigarettes ("e-cigarettes"), which are marketed as an alternative to traditional cigarettes.

2. JUUL reportedly aims to market itself to an adult population of consumers who use nicotine products, advertising JUUL's products as a way to transition from traditional smoking. However, JUUL has recently received heavy criticism that its products were aimed at the youth market.

3. In response to that criticism, JUUL created an action plan to eliminate underage use of their products. To do this, JUUL added extra layers of security to their online purchasing system in order to verify the age of the purchaser. *See JUUL Labs Action Plan* (Nov. 13, 2018), available at https://newsroom.juul.com/juul-labs-action-plan/.

4. When a customer uses JUUL's website, JUUL.com, to complete an online purchase of e-cigarettes or e-cigarette cartridges, he or she must submit detailed information, including name, date of birth, permanent address, and the last four digits of his or her social security number, for age verification.

5. Should a customer opt-out of providing that information, or if the customer's age cannot be verified, the customer may verify his or her age by uploading a real-time photograph, which JUUL uses to match a user's face to an uploaded government-issued Identification Card ("ID").

6. When a customer uploads a photograph and ID, he or she is enrolled in JUUL's facial recognition database(s) using the provided photo, from which JUUL uses third-party facial recognition software to create a scan of his or her facial geometry to match to the provided ID.

7. While many companies that sell age-restricted products, such as tobacco and alcohol, use conventional methods for age verification (such as human review of ID cards), JUUL's customers are required to provide their facial geometry so that JUUL can match that facial geometry data to the ID.

8. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as JUUL – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks or authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

9. Facial geometry features are unique, permanent biometric identifiers associated with each individual. JUUL's use of this technology exposes its customers to serious and irreversible privacy risks. For example, if a database containing facial geometry or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, Facebook/Cambridge Analytica, and Suprema data breaches or misuses – individuals have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

10. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

11. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including handprints, iris scans, and facial photographs – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

12. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018),

available at http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

13. In August 2019 it was widely reported that Suprema, a security company responsible for a web-based biometrics lock system that uses fingerprints and facial geometry scans in 1.5 million locations around the world, maintained biometric data and other personal information on a publicly accessible, unencrypted database. Major Breach Found in Biometrics System Used by Banks, UK police and Defence Firms, The Guardian (Aug. 14, 2019), available at https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

14. In the United States, law enforcement, including the Federal Bureau of Investigation and Immigration and Customs Enforcement, have attempted to turn states' Department of Motor Vehicles databases into biometric data goldmines, using facial recognition technology to scan the faces of thousands of citizens, all without their notice or consent. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post (July 7, 2019), *available at* https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/?noredirect=on&utm_term=.da9afb2472a9.

15. This practice has been criticized by lawmakers. Some states, including Illinois, have refused to comply with law enforcement's invasive requests. *State Denying Facial Recognition Requests*, Jacksonville Journal-Courier (July 9, 2019), *available at* https://www.myjournalcourier.com/news/article/State-denying-facial-recognition-requests-14081967.php.

16. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens' biometrics, such as facial features.

17. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards individuals' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses individuals' biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their facial geometry is collected, stored, and used, as required by BIPA

b. Develop and adhere to a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' facial geometry, as required by BIPA;

c. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate, or otherwise use their facial geometry, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their facial geometry to a third party as required by BIPA.

18. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purposes and length of time for which their facial geometry was being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

19. Upon information and belief, JUUL improperly discloses its customers' facial geometry data to Jumio Corporation and other, currently unknown, third parties, including but not limited to third parties that host biometric data in their data center(s).

20. Upon information and belief, JUUL lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has not and will not destroy their biometric data as required by BIPA.

21. JUUL customers have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, JUUL intentionally interferes with each user's right of possession and control over their valuable, unique, and permanent biometric data.

22. JUUL is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

23. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

24. Plaintiff Jenna Wilkinson is a natural person and a citizen of the State of Illinois.

25. Defendant JUUL Labs, Inc. is a Delaware corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

26. This Court has jurisdiction over Defendant pursuant to 28 U.S.C. §§ 1332(d), 1441, 1446, and 1453(b) because it is subject to the Class Action Fairness Act ("CAFA"), minimal diversity exists, and the amount in controversy exceeds $5 million.

27. Venue is proper in this judicial District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts business within this District and because a substantial part of the events and omissions giving rise to the claims pleaded in this Complaint occurred within this District.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

28. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

29. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

30. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

31. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent

violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

32. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored or used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS 14/15(b).

33. Biometric identifiers include retina and iris scans, voiceprints, fingerprints and scans of hand geometry, and – most importantly here – facial geometry. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

34. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosures. *See* 740 ILCS 14/15(d)(1).

35. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention

schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

36. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at a heightened risk for identity theft and left without any recourse.

37. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics. BIPA also protects individuals' rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed, allowing individuals to make a truly informed choice. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

38. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendant Violates the Biometric Information Privacy Act.

39. By the time BIPA passed through the Illinois Legislature in mid-2008, most companies who had experimented with using customers' biometric data stopped doing so.

40. However, JUUL failed to take note of the shift in Illinois law governing the collection, use, storage, and dissemination of biometric data. As a result, Defendant continues to collect, store, use and disseminate individuals' biometric data in violation of BIPA.

41. Specifically, when customers endeavor to make an online purchase from Defendant, Defendant requires them to have their facial geometry scanned to enroll them in JUUL's database(s).

42. JUUL uses customers' facial geometry as an age verification method.

43. Defendant fails to inform individuals of the purposes and duration for which it collects, stores, and uses their facial geometry data; fails to inform customers that it discloses or disclosed their facial geometry data to currently unknown third parties, which host the biometric data in their data centers; and, fails to obtain written releases from individuals before collecting their facial geometry, as required by BIPA.

44. At no time did JUUL secure written releases from individuals before collecting their facial geometry.

45. Furthermore, Defendant fails to publish a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying individuals' facial geometry data when the initial purpose for collecting or obtaining their facial geometry is no longer relevant, as required by BIPA.

46. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlight why such conduct – where individuals are aware that they are providing biometric data, but not aware of to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as one's facial geometry,

who exactly is collecting their biometric data, where it will be transmitted, for what purposes, and for how long. Defendant disregards these obligations and their customers' statutory rights and instead unlawfully collect, store, use and disseminate their customers' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

47. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

48. Plaintiff and others similarly situated are not told what might happen to their biometric data if and when Defendant merges with another company, or worse, if and when Defendant's business folds, or when the other third parties that have received individuals' biometric data businesses fold.

49. Since Defendant neither publishes a BIPA-mandated data retention policy nor discloses the purposes for its collection and use of biometric data, individuals have no idea the extent to whom Defendant sells, discloses, rediscloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

50. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

51. By and through the actions detailed above, Defendant disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Jenna Wilkinson's Experience.

52. On or about July 15, 2018, Plaintiff Jenna Wilkinson made an online purchase of JUUL products directly from Defendant's website.

53. JUUL required Plaintiff to submit a photograph of her face in order to match it against an uploaded image of Plaintiff's ID card.

54. In order to match the photograph against the ID card, Defendant created a scan of Plaintiff's facial geometry, and Defendant subsequently stored Plaintiff's facial geometry data in its database(s).

55. Plaintiff was never informed of the specific limited purposes or length of time for which Defendant collects, stores, uses and/or disseminates her biometric data.

56. Plaintiff has no knowledge of any biometric data retention policy developed by Defendant and made available to the public, nor does she know whether JUUL will ever permanently delete her biometric data.

57. Plaintiff has never been provided with nor ever signed a written release allowing Defendant to collect, store, use or disseminate her biometric data.

58. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's multiple violations of BIPA alleged herein.

59. No amount of time or money can compensate Plaintiff if her biometric data is compromised by the lax procedures through which Defendant captured, stored, used, and disseminated her and other similarly-situated individuals' biometrics. Moreover, Plaintiff would not have provided her biometric data to Defendant if she had known that Defendant would retain such information for an indefinite period of time without her consent.

60. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

61. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40. Nonetheless, Plaintiff is aggrieved because she suffered an injury-in-fact based on Defendant's violations of her legal rights. Defendant has intentionally interfered with Plaintiff's right to possess and control her own sensitive biometric data. Additionally, Plaintiff suffered an invasion of a legally protected interest when Defendant secured her personal and private biometric data at a time when it had no right to do so, a gross invasion of her right to privacy. BIPA protects consumers like Flores from this precise conduct. Defendant had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

62. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow.

63. Plaintiff also suffered an informational injury because Defendant has failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature has created a right: a consumer's right to receive certain information prior to a company securing his or her highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.

64. Plaintiff also suffered an injury in fact because Defendant has improperly disseminated her biometric identifiers and/or biometric information to third parties that hosted the biometric data in their data centers, in violation of BIPA.

65. Pursuant to 740 ILCS § 14/15(b), Plaintiff was entitled to receive certain information prior to Defendant securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which Defendant collects, stores, uses and disseminates her private biometric data; information regarding Defendant's biometric retention policy; and a written release allowing Defendant to collect, store, use, and disseminate her private biometric data. By depriving Plaintiff of this information, Defendant injured her. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

66. Plaintiff has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining compensation as a result of being denied access to material information about Defendant's policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties; in the form of interference with her right to control and possess her confidential biometric data; and, in the form of the exposure to substantial and irreversible loss of privacy.

67. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

68. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings claims on her own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

69. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it ***first*** (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose(s) and length of time for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS 14/15.

70. Plaintiff seeks class certification under Rule 23(b) of the Federal Rules of Civil Procedure for the following class of similarly-situated individuals under BIPA:

> All customers of Defendant in the State of Illinois who had their facial geometry collected, captured, received, otherwise obtained, maintained, stored, or disclosed by Defendant during the applicable statutory period.

71. This action is properly maintained as a class action under Rule 23(b) because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. Plaintiff's claims are typical of the claims of the class; and,

D. Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

72. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from JUUL's records.

Commonality

73. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured, maintained, stored or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or redisclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's and the putative Class' biometric data will be unlawfully accessed by third parties;

I. Whether Defendant used Plaintiff's and the Class's facial geometry to identify them;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally or recklessly.

74. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

75. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

76. The claims asserted by Plaintiff are typical of the class members he seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

77. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim. However, if any such class member should become known, he or she can "opt out" of this action pursuant to Rule 23.

Predominance and Superiority

78. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number

of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

79. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

80. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

81. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

82. Defendant fails to comply with these BIPA mandates.

83. Defendant is a Delaware corporation registered to do business in Illinois and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

84. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

85. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

86. Defendant failed to publish a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

87. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and has not and will not destroy Plaintiff's or the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

88. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

89. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

90. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] ***first***: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

91. Defendant fails to comply with these BIPA mandates.

92. Defendant is a Delaware corporation registered to do business in Illinois and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

93. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

94. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

95. Defendant systematically and automatically collected, captured, received through trade, or otherwise obtained Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

96. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, received through trade, or otherwise obtained, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

97. By collecting, capturing, receiving through trade, or otherwise obtaining Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

98. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

99. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

100. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

101. Defendant fails to comply with this BIPA mandate.

102. Defendant is a Delaware corporation registered to do business in Illinois and, therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

103. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their facial geometry), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

104. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

105. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

106. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

107. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Jenna Wilkinson respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Jenna Wilkinson as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

Date: June 24, 2020

Respectfully Submitted,

/s/ Haley R. Jenkins

Ryan F. Stephan
James B. Zouras
Haley R. Jenkins
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza, Suite 2150
Chicago, Illinois 60606
312.233.1550 | 312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
hjenkins@stephanzouras.com

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on June 24, 2020, I filed the attached with the Clerk of the Court using the ECF system, which will send such filing to all attorneys of record.

/s/ Haley R. Jenkins